UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/466,625	12/17/1999	RONALD P. DOYLE	RSW990077	1396

7590   03/24/2004

JEANINE S RAY-YARLETTS
IBM CORP DEPT T81/BLDG 062
PO BOX 12195
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER
WU, ALLEN S

ART UNIT	PAPER NUMBER
2135	5

DATE MAILED: 03/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
	09/466,625	DOYLE ET AL.
Office Action Summary	Examiner	Art Unit	
	Allen S. Wu	2135	

-- The MAILING DATE of this communication appears on the cov r sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 January 2004*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8, 10-17, 19-26, and 28-33* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *8,17 and 26-33* is/are allowed.

6)☒ Claim(s) *1-7, 10-16, and 19-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 December 1999* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   This action is in response to applicant's amendment filed 7 January 2004. The

applicant has canceled claims 9, 18, and 27.

Allowable Subject Matter

2.   Claims 8, 17, 26, and 28-33 are allowed.

3.   The following is a statement of reasons for the indication of allowable subject

matter:

> The closest cited prior art (U.S. Patent No. 6,067,623) fails to teach or
>
> suggest the features of sending and receiving a log-on message using
>
> placeholder syntax in place of a user identifier and a password for transparently
>
> logging a user on to a secure legacy host application recited by independent
>
> claims 8, 17, 26 and 33. Claims 28-32 would also be allowable for the reasons
>
> stated above.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1-7, 10-16, and 19-25 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Blakley, III et al (hereinafter Blakley), US Patent 6,067,623, in view of

Thompson, Safety in Cyberspace: Planning Effective Web-to-Host Access Security.

As per claims 1, 10, and 19, Blakley discloses providing end-to-end user

authentication for legacy systems (Enterprise resources, abstract and col 3 ln 51-

58) comprising: establishing a secure session from a client machine to a server

machine using a digital certificate, transmitted from said client machine to said

server machine, wherein said digital certificate represents said client machine or

user thereof (client certificate, col 4 ln 18-64); establishing a session from said

server machine to a system on behalf of said client machine, responsive to

establishment of said secure session (col 4 ln 18-66 and fig 1).

Blakley does not explicitly teach storing a digital certificate at said server

machine. However, Blakley discloses use of the need of reducing client/server

communications (col 1 ln 53-67). The method of storing data on a server for later

use is well known in the art for eliminating further communication between a

client and a server for obtaining the same information. It would have been

obvious to one of ordinary skill in the art to modify the teachings of Blakley to

further store the received digital certificate for later authentication of the client

because it would have decreased network traffic.

Blakley does not explicitly teach passing said stored digital certificate to a

host access security system. However, Blakley discloses the possibility of using

more than three tiers (col 4 ln 12-17) and that authentication can be performed

by an external security server (col 4 ln 67-col 5 ln 6). Furthermore, Blakely discloses using user supplied credential, which may be a client certificate, for obtaining access credentials (col 4 ln 18-65), including a user identifier associated with said located access credentials and either a stored password or a generated password substitute (col 4l ln 19-41 and col 4 ln 60-col 5 ln 16). Therefore, one of ordinary skill in the art would have been able to modify the teachings of Blakley to include a host access security system for using a digital certificate (passed credentials) to locate access credentials for said user and further return from said host access security system to server machine, a user identifier associated with said located access credentials and either a stored password or generated password substitute representing said located credentials. In such a modification, passing a stored digital certificate from a server machine to host access security system is inherent to obtaining such user credentials for authentication of client.

Furthermore, Blakely does not explicitly teach the server sending a stored certificate from said server machine to a host access security system, responsive to receiving, at said server machine, a request from said host system for log-on information of said user. However, Blakely discloses authenticating the client in response to a request by the client (col 4 ln 50-65). Both are means of initiating an authentication scheme for client access credentials. One of ordinary skill in the art at the time of the applicant's invention would have been able to modify the teachings of Blakely authentication being initiated in response to receiving a

request from a host system (back end) since the applicant has not explicitly

stated any particular use for such a response other than initiating an

authentication scheme and that a request from a client is just as efficient.

Blakely further discloses transparent logging of said user to a legacy

system (enterprise resource, col 5 ln 17-31), wherein no change is required for

the legacy system (col 6 ln 7-19) and legacy system authentication is

accomplished through a secondary login mechanism (col 6 ln 7-11). Blakely

does not explicitly teach authentication at a host system for a legacy host

application. Thompson discloses a host legacy system, which uses a supplied

use rid and password to logon the client (page 3 paragraph 4) wherein a multi-

tier architecture is employed (page 3 paragraph 6 – page 4 paragraph 3). Both

Thompson and Blakely disclose methods of providing authentication to legacy

applications (enterprise resources). Thompson further discloses different logon

logic for different enterprise resources. Therefore, one of ordinary skill in the art

would have been able to modify the logon logic of Thompson to forward the user

identifier and password such that said forwarded user identifier and password

can be used by said host system to transparently log said user on to a secure

legacy host application executing at said host system, without requiring change

to said host system. It would have been obvious to one of ordinary skill in the art

at the time of the applicant's invention to combine the teachings of Thompson

within the system of Blakely to further include a client authentication scheme to a

host system because of the trend of enterprise information residing on mainframe

host systems and a need to protect the enterprise information on such host systems (see Thompson page 1).

Furthermore, Blakely discloses communication between a server and a legacy system (col 3 ln 51-58 and col 5 ln 49-61). Furthermore, in the modification of including authentication to legacy host systems, a legacy host communication protocol is inherently needed to provide communication between heterogeneous systems, specifically between a host and server in the multi-tier communication setup (see Thompson page 3 paragraph 3).

As per claims 2, 11 and 20, Blakely discloses a digital certificate as described above (see claim 1). Blakely does not explicitly teach a digital certificate being an X.509 certificate. Thompson discloses a X.509 digital certificate for strong authentication of clients (page 2 paragraph 5). It would have been obvious to one of ordinary skill in the art to modify the certificate of Blakely teachings to be an X.509 certificate because the X.509 certificate is well known in the art to provide a standard for strong authentication based on different user information encapsulated in the certificate.

As per claims 3, 12, and 21, Blakely discloses communication between a server and a legacy system as described above (see claim 1). However, Blakely does not explicitly teach a 3270 emulation protocol. Thompson discloses such an emulation protocol (page 3 paragraph 3) as a communication protocol.

As per claims 4, 13, and 22, Blakely discloses communication between a

server and a legacy system as described above (see claim 1). However, Blakely

does not explicitly teach a 5250 emulation protocol. Thompson discloses such

an emulation protocol (page 3 paragraph 3) as a communication protocol.

As per claims 5, 14, and 23, Blakely discloses communication between a

server and a legacy system as described above (see claim 1). However, Blakely

does not explicitly teach a virtual terminal protocol. Virtual terminal protocols are

well known in the art, such as the TELNET communication protocol. It would

have been an obvious to one of ordinary skill in the art at the time of the

applicant's invention to modify the combination of Blakely and Thompson to use

a virtual terminal protocol as an alternative means of communication between the

server and host.

As per claims 6, 15, and 24, Blakely discloses an access security system

(as described in claim 1). However, Blakely does not explicitly teach a host

access security system being a Resource Access Control Facility system.

Thompson discloses such a system (page 2 paragraph 3). RACF is well known

in the art to provide client authentication to host systems. It would have been

obvious to one of ordinary skill in the art at the time of the applicant's invention to

use a RACF system as a host access security system due to its trustworthiness

of authentication (see Thompson page 2 paragraph 3) and the advantage of using the same security system to access credentials as the one used by the host system to eliminate the use of another external security system.

As per claims 7, 16, and 25, Blakely discloses a Web application server machine (col 5 ln 49-61).

Response to Arguments

6.   Examiner notes applicant has intended to submit a proposed replacement drawing for Fig. 6 (page 19 of remarks). However, the replacement drawings are missing from the file. The examiner respectfully requests resubmission of the replacement drawings in the next correspondence to the office.

7.   Applicant's arguments with respect to claim1-7, 10-16, and 19-25 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

8.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure

US Patent 6,275,941, to Saito et al, discloses user authentication a credential access using a digital certificate.

US Patent 6,052,785, to Lin et al, discloses user authentication to a host system in a multitiered network.

US Patent 6,556,995, to Child et al, discloses transparent user logon to a database.

9.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.
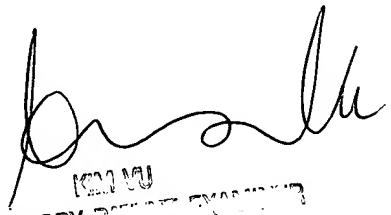
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Allen Wu
Patent Examiner
Art Unit 2135

ASW